Security in knowledge

SOCIAL MEDIA IN MARKETING AND THE WORKPLACE: LEGAL AND REGULATORY COMPLIANCE

David M. Adler

Leavens, Strand, Glover & Adler LLC

Behnam Dayanim

Paul Hastings LLP

RSA CONFERENCE 2013

Session ID: LAW T19

Session Classification: General Interest

Agenda

- Advertising and Marketing
- Data Privacy in Social Media
- Copyright and Trademark
- Employer-Employee issues (liability and enforcement)
- Drafting an effective Social Media policy for your company and Monitoring channels/compliance

Advertising & New Media

- **Communications Decency Act of 1996**
- Core of act invalidated, but key provisions remained
- Immunity for content or for removing "objectionable" content
- "No provider or user of an *interactive computer service* shall be treated as the *publisher or speaker* of any information *provided by* another information content provider."
- Changes traditional rules applicable to (offline) media publishers

Advertising & New Media: CDA

- "Interactive Computer Service" includes social networking sites such as MySpace, ISPs such as America Online, and commercial websites with third-party content, bulletin boards, blogs, etc.
- Example: A YouTube post inaccurately criticizes a company or product
  - YouTube bears no liability
  - Must identify and sue poster
  - May be able to persuade YouTube voluntarily to remove post, but, absent trade secret, copyright or similar exigency, no obligation to do so
  - May have to subpoena to obtain poster information

Advertising & New Media: CDA

- **Limitations?**
  - Only defamation/obscenity, or broader than that?
    - Any liability that stems from status as publisher, speaker, distributor
    - Does not expand or limit intellectual property laws
  - Content must be "provided by" another content provider
  - Not applicable if "responsible, in whole or in part, for the creation or development" of the content
    - Cannot solicit or encourage what is specifically objectionable about the content
    - Addition of titles, headers, pull-outs, logos?

Advertising & New Media: Endorsements

- Three Basic Principles from FTC Endorsement Guide:
  - Endorsements must be truthful and not misleading;
  - Material connections must be disclosed; and
  - Ad must clearly and conspicuously disclose the generally expected results in the depicted circumstances.
- Advertisers subject to liability for statements made by endorsers

Advertising & New Media: Endorsements

- Social Media
  - Fundamental question is whether, viewed objectively, the relationship between the advertiser and the speaker is such that the speaker's statement can be considered "sponsored" by the advertiser and therefore an "advertising message."
  - **Lack of control** over a specific statement made via new forms of consumer-generated media **does not necessarily mean** that the advertiser is not responsible for the content.
- Must monitor social media sites **and need action plan**
- Avoid appearance that company implicitly adopts statements it knows are not supported

Advertising & New Media: Endorsements

- Enforcement Actions
  - Spokeo (June 2012)
    - $800,000 settlement
    - FCRA violations involved the collection of data from social networking sites used for employment screening
    - Endorsement guideline violations involved endorsements posted on news and tech websites and blogs
      - Although supposedly "independent," the endorsements were actually written by Spokeo employees at the direction of the company
  - Legacy Learning Systems (March 2011)
  - Reverb Communications (August 2010)

Advertising & New Media: Endorsements

- Tensions with CDA: when is the company responsible?
- Stacey Ferguson, FTC Div of Adv Practices, Dec. 2009
  - *Q: What about sites that allow you to review the product on the advertiser's site? Consumer buys product and writes: this is the greatest ever, it cured my skin disorder. Is the advertiser who puts up the site responsible for the content?*
  - *Ferguson: **Not entirely resolved**. If it's a statement on behalf of the company, the company would be responsible. But if the consumer is making her statement on her own, but it's on the company's site, that's a gray area. The CDA would exempt the person who owns the website from responsibility for content on the site. But if the advertiser knows the representation isn't substantiated, the advertiser should be wary of keeping the statement on the site.*

Advertising & New Media: Affiliate Marketing

- Third parties – *e.g.*, website operators or individuals – who drive traffic to a website in exchange for a commission
- FTC concerned that affiliates are using improper means – *e.g.*, false and deceptive claims, fake blogs, failing to disclose material contacts
  - Acai Berry Settlements (2011-2012)
    - FTC launched first action against "affiliate networks" for use of fake news sites to promote the weight loss effects of acai berries
    - Filed charges against ~10 affiliates, including IMM Interactive/Coapeac, which paid **$1.3 million** in fines for operating the fake websites and recruiting a network of affiliates and Coleadium, Inc., which paid **$1 million** for entering into contracts with affiliates for similar fake websites

Advertising & New Media: Mobile Marketing

- Increased focus; team at FTC devoted to monitoring mobile advertising
- 2 enforcement actions for mobile apps of note:
  - W3 Innovations' "Emily's World" Apps
    - W3 agreed to pay $50k
    - Notable as first "App case" and for uptick in COPPA actions & revised COPPA rule
  - "AcneApp" and "Acne Power" Apps
    - Marketer cited to a bogus journal article and provided endorsements
    - Companies involved agreed to pay $14k and $1700 respectively

Data Privacy

- Three hot-button issues
- Mobile privacy
  - Location information?
  - Medical/Financial?
- Children's privacy
  - First update to Children's Online Privacy Protection Act rules in 12 years
- Access to employees' and job applicants' personal social media

Mobile Privacy

- FTC issued report regarding mobile apps for kids in February (labeling them dis*app*ointing) and general guidelines for how to market a mobile app in August
- General guidelines include
  - Tell the truth about what your app can do
  - Disclose key information clearly and conspicuously
  - Build in privacy considerations from the start
  - Be transparent about practices
  - Offer choices that are easy to find and use
  - Honor privacy promises
  - Protect kids' privacy
  - Collect sensitive info only with consent
- Preference for transaction-based notice and choice

Mobile Privacy

- California enforcement activity
  - In October, the CA AG sent warning letters regarding 100 different mobile apps, including Delta, United and OpenTable
  - Demanded privacy policies in apps
- In December, she filed suit against Delta
  - Suit recognizes open question of whether a website policy can suffice even for mobile app, but notes that the Delta website policy does not mention the mobile app
  - Complaint seeks $2500 per violation under CA Online Privacy Protection Act and characterizes each download as a violation
- In January, California AG issued a mobile privacy recommendations report
  - Framed as "common sense" recommendations
  - Recognized that recos go beyond current law

Children's Privacy

- After 12 years, the FTC revised its rule implementing the Children's Online Privacy Protection Act (protects kids under 13)
  - Scope has been expanded:
    - Continues to cover sites/apps directed to kids or that know they have kids' information and sites/apps that have content that appeals to kids
    - Now includes vendors such as ad networks or app plug-ins, if they know they are collecting kids' information from another website or service
    - Also includes services that are "directed" to kids but that don't target them as primary audience (unless they verify age and bounce kids)
    - Revises definition of "personal information" to include geolocation information, photos, videos, audio files and persistent identifiers
  - Other changes include voluntary approval process for consent mechanisms and stronger data security provisions

Requiring Access to Social Media

- Electronic Communications Privacy Act imposes limitations on access to stored communications (and interception)
  - Limits provider's ability to disclose communications
- BUT says nothing about compelling subscriber directly
  - At least one court had upheld orders requiring such consent
- Issue has been percolating for some time
  - municipality in Idaho in interviews of job applicants was first reported incident
  - More recently, incident involving correctional authorities in Maryland
  - University athletic departments and scholarship athletes (requiring athlete to "friend" a monitor)

Requiring Access to Social Media

- States and Congress have considered "bullet bills" to prevent
  - Six states – California, Delaware, Illinois, Maryland, Michigan and New Jersey – passed laws (all in 2012) prohibiting requirement to disclose a user name or password for a personal social media account
  - California, Delaware Michigan and New Jersey also apply to academic institutions and students
  - Congress is considering similar legislation
- These types of laws must grapple with real concerns
  - National security?
  - Gang affiliations?

Legal Risks: Intellectual Property

- Copyright
  - Practical Applications
    - Use of a Photo: Agence France Presse v. Morel, U.S. District Court for the Southern District of New York, No. 10-02730
- Trademark
- Trade Secrets
  - *Christou* v. *Beatport*: unfair comp case between a night club owner and one of his former partners
  - If primary "value" of an account is the list of "followers" publicly available list is, therefore, not a secret
  - treat the login credentials as the trade secret since this control's access & communication

Legal Risks: Practical Applications

- Litigation
  - Jury Pool
- Prospective Employees
  - New Laws about Social Media Passwords
- Disclosure of Private Information

Legal Risks: Practical Applications

- Securing Social Media Accounts
  - Whose Account is it Anyway?
    - Employer should create the account
  - Contractual Definitions
    - Include explicit ownership provisions in employment agreements
    - "Accounts are exclusive property of the company & employee has no ownership"
    - Public Monitoring
    - Immediate Termination of access for departing employee

What Should You Do?

- There are steps you can take
- Focus on relevant markets
- Adopt internal rules/policies and monitoring
- Contractual provisions
- Awareness – education

Practical Guidelines

Types of Rules and Monitoring to Consider

- Ensure that all employees know the ins and outs of social media and the risks and legal consequences associated
- Make yourself known! Proper disclosures of affiliations & compensation are key
- Understand the Company's privacy policy and the type of data collected from consumers
  - Dynamics are changing quickly
  - Discuss collection and retention policies with in-house or outside counsel
- Make sure you have received consent where necessary (e.g., text messages)

Practical Guidelines

Types of Rules and Monitoring to Consider

- Endorsement monitoring
  - Reasonable program; scope depends on risk of deception and harm
  - Train members of "network" what they can and cannot say about the product (e.g., proven benefits of product, financial relationship!);
  - Set up a reasonable monitoring program to check on what your "network" is saying;
  - Follow up if you find questionable practices.
- While applicability of the CDA to comments posted on a Company website is unclear, Company should be "wary" of an unsubstantiated claim posted on a Company website

Practical Guidelines

- Action Items
  - Proper Contractual Provisions
  - Code of Ethics/Code of Conduct
  - Social Media Policy
  - Monitoring
    - Google Alerts
      - Brand names/Trademarks
      - Social Media Handles
      - Executives Names
    - Facebook/Myspace/LinkedIn Pages
  - Updated Privacy Policy

Workplace Trends

- On May 30, 2012 NLRB General Counsel (GC) 3d Memo
- Of the 7 Policies reviewed, 6 unenforceable
- Key Take-Aways:
  - 🚫 Admonition to "**Use technology appropriately**" & not **"release confidential guest, team member or company information"**
  - 🚫 Instructions to ensure posts are **"completely accurate and not misleading and that they do not reveal non-public information on any public site"**
  - 🚫 Prohibition to not **"reveal non-public company information on any public site"**

Workplace Trends

- More Key Take-Aways
  - 🚫 Health care provider's prohibition against revealing "**personal information** about employees, customers, customers' patients **via social media**
  - 🚫 Requirement that employees **get permission before using third-party content**
  - 🚫 Savings clause that **"Policy will not be construed or applied in a manner that improperly interferes with employees' rights under the National Labor Relations Act"**

Workplace Trends

- Key Take-Aways Con't:
  - Admonition to respect copyright (& other IP) is OK as long as policy does not require an employee to seek permission
  - Policies "that clarify and restrict their scope by including examples of clearly illegal or unprotected conduct, such that they would not reasonably be construed to cover protected activity, are not unlawful."

Workplace Trends

- Key Take-Aways Cont:
  - Employee Disciplinary Actions. Disciplining an employee is lawful if:
    - (1) the posting does not address the terms or conditions of employment;
    - (2) the employee acted alone in making the social media posting; or
    - (3) the posting is deemed to be egregious and offensive
  - Avoid vague and overly broad terms.
    - Limit language and context to clarify that the policy does not prohibit employee discussions of the terms and conditions of employment.
  - Give specific examples of prohibited behavior.

Practical Guidelines

- Here's what to include in your Social Media Policy:
  - **Philosophy:** how does social media fit into an employees job expectations and performance
  - **Behavioral Expectations:** areas of expertise; respectful conduct; timeliness; perspective; transparency & judiciousness
  - **Channel expectations:** Which sites (communication channels) are appropriate for which types of communications.
  - **Contextual Expectations:** conversational style; perception; value
  - **Content Expectations:** use of company proprietary information, including current projects, trademarks, names, logos